**Findings:**

ICANN’s current treatment of privacy and proxy services lacks clarity, and has resulted in unpredictable outcomes for stakeholders. In terms of the review team’s scope:

* law enforcement agencies have advised that the current privacy/proxy services situation does not meet their legitimate needs;
* stakeholder feedback suggests that on balance consumer trust is being harmed rather than promoted (including the trust of consumers of privacy and proxy services, who have little or no certainty about how their data will be treated); and
* the current use of privacy and proxy services raises questions about whether ICANN is meeting its AoC commitments relating to ‘timely, unrestricted and public access’ to WHOIS data.

At the same time, the review team recognizes that:

* there is strong consumer demand for privacy and proxy services;
* privacy and proxy services can be used to address legitimate legal and commercial interests; and
* with appropriate regulation and oversight, these services appears capable of addressing stakeholder needs.

**Recommendation:**

The Review Team recommends that ICANN should initiate processes to regulate and oversee privacy and proxy service providers.

ICANN should develop these processes in consultation with all interested stakeholders.

If appropriate, this could include a review of existing practices used by proxy/privacy service providers.

The review team considered that one possible approach to achieving this would be to establish, through the appropriate means, an accreditation system for all proxy/privacy service providers. As part of this process, ICANN should consider the merits (if any) of establishing or maintaining a distinction between privacy and proxy services.

The goal of this process should be to provide clear, consistent and enforceable requirements for the operation of these services consistent with national laws, and to strike an appropriate balance between stakeholders with competing but legitimate interests. At a minimum, this would include privacy, law enforcement and the industry around law enforcement.

ICANN could, for example, use a mix of incentives and graduated sanctions to encourage proxy/privacy service providers to become accredited, and to ensure that registrars do not knowingly accept registrations from unaccredited providers.

ICANN could develop a graduated and enforceable series of penalties for proxy/privacy service providers who violate the requirements, with a clear path to de-accreditation for repeat, serial or otherwise serious breaches.

In developing the process to regulate and oversee privacy/proxy service providers, consideration should be given to the following objectives:

* Clearly labeling WHOIS entries to indicate that registrations have been made by a privacy or proxy service
* Providing full WHOIS contact details, which are contactable and responsive
* Adopting agreed standardized relay and reveal processes and timeframes (these should be clearly published, and pro-actively advised to potential users of these service so they can make informed choices based on their individual circumstances)
* Registrars should disclose their relationship with any proxy/privacy service provider
* Maintaining dedicated abuse points of contact for each provider
* Conducting periodic due diligence checks on customer contact information
* Maintaining the privacy and integrity of registrations in the event that major problems arise with a privacy/proxy provider

Finally, for the avoidance of doubt, the WHOIS policy, referred to in Recommendation 1 above, could include an affirmative statement that clarifies that ICANN regards the registered name holder in the WHOIS data to be the entity that obtains all rights and assumes all responsibility for the domain name and its manner of use.